SysAdmin's Notebook

Fortinet SysAdmin's Toolkit

Overview

No computer or network system is ever completely self-sufficient or self-contained. Even systems that appear to be perfect—when everything is working smoothly and no changes are being made—will eventually need help: something will need to be fixed, reconfigured, reinstalled, or tested. Just like an auto-mechanic has a favorite socket set and screwdrivers, SysAdmins also have their toolkits with their preferred tools.

Each SysAdmin builds up their toolkit based on their experience and what they are maintaining. Almost every SysAdmin admits that, at least one time, they needed a tool to get something done and didn't have it with them. When a device like a firewall breaks speed in getting it up and working properly again is usually the highest priority. This is not a good time to find out you don't have one of the tools you need.

SysAdmins build up a set of tools, both physical and digital, that help them fix problems or generally make their lives easier when dealing with the foibles of the Information Age. This document describes a list of tools that I have found useful while diagnosing and fixing Fortinet products. The tools listed below are ones that I have found useful in my personal experience, and includes tools recommended by others.

This document includes information on:

- **Hardware**
- **Software**
- **Online Resources**

Don't forget to print out our **Toolkit Checklist** to keep track of your tools!

About the Fortinet SysAdmin Toolkit:

Here are a few things you should know about the Fortinet SysAdmin Toolkit.

Frequent changes

Expect this document to be constantly updated.

No endorsements

While I have preferences, these are not recommendations of one product over another but simply possible options for you to check out yourself. I do not endorse one product over any other. I include them because I've tried them and they have worked for me. If your favorite is not listed send an email to techdocs@fortinet.com, and I'll try to check it out.

Hardware

The hardware items listed are fairly generic. Go by your own experience with quality when possible. I haven't tested every possible brand and model out there, and even if I could product quality can change over time.

Software

I have listed some specific software, websites and utilities. Whenever I am aware of multiple options I try to list them.

Just the cheap stuff

I know few SysAdmins with a large budget, so when possible, I point to free software or items that are inexpensive. If you do have a large budget why waste it on things you don't have to spend a lot of money on?

Not just for Fortinet products

I include a few things that would be useful in any networking environment, because sometimes you have to make Fortinet products work in an existing network

Make a list

Some of the items listed come with Fortinet products, but I've included them so that this document can be used as a "Toolkit checklist" to make sure that you have all of your equipment. In fact, I've included a checklist at the end.

Hardware

Console Cable

Many Fortinet appliances have a console port of some kind for directly accessing the device. There are some variations in the connection ports, but the most common one is an RJ-45 Console port. The stock cable that comes with these devices is a DB-9 Serial connector to RJ-45 connector. It seems that these cables are constantly getting misplaced so if you come across an extra one don't throw it out.
The pinning of console cables is not universal between vendors, but Fortinet shares the same pinning sequence as Cisco, so you can use any old Cisco console cables that you may have lying around.

USB to Serial Adapter

Finding a port to plug in a standard console cable is getting difficult. Fewer computers are coming with a R-232 serial connection as a standard port. Finding one built in to a laptop built in the last few years is almost unheard of. One solution is to carry a USB to Serial adapter.

Ethernet Cables

Having a few extra Ethernet cables around is always a good idea for testing. Sometimes it is worth the few minutes it takes to verify whether or not a faulty cable is the issue. Swapping with a known good cable is a lot cheaper than one of those fancy and expensive cable testers.
Most Ethernet cables tend to be of a length for connecting a computer to a wall socket or switch (7 feet or longer), but sometimes you will want a few in the size range of 1 foot or less (such as when performing an HQIP test because they are making connections to the interfaces of the same device).

Crossover Ethernet Cable

Many Ethernet interfaces these days are equipped with autosensing or switchable uplink ports that automatically switch between MDI and MDIX modes, but it is not universal– some older devices may need to use a crossover cable. It doesn't take up much space to have a short crossover cable; just in case.
If you have a crimping tool and some empty RJ-45 connectors you can build your own crossover cable. There are websites that have the instructions or at least wiring maps:

- http://www.makeuseof.com/tag/ethernet-crossover-cable/
- http://www.littlewhitedog.com/content-8.html
- http://www.incentre.net/ethernet-wiring-diag.html

Serial to Ethernet Adapter

This is one of those pieces that you may never need but is fairly inexpensive and if you ever need it you will be glad you have it. The console cable that comes with Fortinet units is a few feet long and will work in most cases, but the layout of some data centers make it awkward to be right next to a device, especially if you're going to be there a long time and would like access to a desk. This adapter will enable you to turn any Ethernet cable into a console cable.
For the pinning instructions to make sure the adapter is compatible with Fortinet products follow the instructions found at:
http://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=11344&sliceId=1&docTypeID=DT_KCARTICLE_1_1&dialogID=14777742&stateId=0

RJ-45 Ethernet Straight Through Coupler

This little device doesn't cost much and is available in multipacks for a few dollars. You don't want to use them as a permanent part of your infrastructure, but they can be quite useful for temporary solutions.

- When you don't have a single cable long enough you can combine two cables to reach the length.
- When combined with a short crossover cable you can convert a long straight through cable to a crossover.
- If you don't have a serial to Ethernet adapter you can extend the length of a console cable.

USB Cables

In addition to the standard console ports a number of models of Fortinet products are also equipped with USB MGMT ports. With the FortiExplorer software and the correct USB cable you can manage these devices using either the CLI or the Web-based Management tool without needing to know the IP address of the device or the parameters required to set up a console connection. The types of USB connection ports in use are:

USB Standard B

USB Mini-B

Software

Text/Code Editor

When choosing an editor it is best to choose a code editor over one that is designed just for text, such as Window Notepad. The primary function with Fortinet products is to view or edit configuration files. A code editor will work better with the indents and other formatting that is particular to code files, even if they are essentially just text. This helps to make looking at the code more intuitive. Note that text editors can include some unwanted information when saving the file.

Notepad++

Platform: Windows
Price: Free
Available for download at:
http://notepad-plus-plus.org/

TextWrangler

Platform: Mac OS
Price: Free
Available for download at:
http://www.barebones.com/products/textwrangler/

Terminal Emulation

While the Web-based Manager does have a CLI widget, I get better performance and more versatility when using Terminal Emulation software. If you are using the console connection to access the BIOS of the device the CLI widget will not be available.

Putty

Platform: Windows
Price: Free
Available for download at:
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

Terminal

Platform: Mac OS
Price: Free
Available as a built-in component of the Operating System

TFTP Server

TFTP is a file transfer protocol noted for its simplicity and small memory footprint. It is commonly used as a method of uploading files to devices that do not have a lot of memory or store a lot of data such as network devices.

- If the TFTP server does not appear to work, the first step is to make sure that some other service or application is not using port 69.
- Whenever using the TFTP server, it is also important to turn off any software firewalls running on the computer acting as the server.

Tftpd32

Platform: Windows
Price: Free
Available for download at:
http://tftpd32.jounin.net/tftpd32_download.html

Solarwinds TFTP Server

Platform: Windows
Price: Free
Available for download at:
http://www.solarwinds.com/products/freetools/free_tftp_server.aspx

TFTP Server

Platform: Mac OS
Price: Free
Available for download at:
http://ww2.unime.it/flr/tftpserver/

MD5 Checking Tool

MD5 is a widely used cryptographic hash function that is used to verify the integrity of downloads such as the Fortinet firmware files. To make sure the download process has given you a clean uncorrupted file to install, you can compare the MD5 value listed on the site for each downloadable file and compare it to the results of an MD5 scan of the file after you have downloaded it.

WinMD5Free

Platform: Windows
Price: Free
Available for download at:
http://www.winmd5.com/

LDAP Browsing Tool

LDAP walking or browsing tools are useful when working with LDAP authentication in that they can more intuitively find the long strings used to describe the identity objects within an LDAP server's database.

LDP.exe

Ldp.exe is a Windows 2000 Support Tools utility you can use to perform Lightweight Directory Access Protocol (LDAP) searches against the Active Directory for specific information given search criteria.
Platform: Windows
Price: Free
Available for download as part of the Windows Server toolkit:
http://www.microsoft.com/en-us/download/details.aspx?id=15326
Available for download as an individual file:
www.computerperformance.co.uk/ScriptsGuy/ldp.zip
Instructions for use available at:
http://support.microsoft.com/kb/224543

Packet Sniffing Software

Packet sniffing software is used to analyze the individual packets traveling across the network to get a more granular view of what is happening with the traffic for troubleshooting purposes.

Wireshark

Wireshark is a free and open-source packet analyzer.
Platform: Windows, Mac, Linux, BSD and Solaris
Price: Free
Available for download at:
http://www.wireshark.org/download.html

Online Resources

With the exception of the actual Fortinet sites, the online sites, services and utilities provided in this document are not recommendations by Fortinet, but examples. Whenever possible, I've tried to list more than one.

Useful Fortinet Sites for Technical Information

- Fortinet Technical Documentation Site: http://docs.fortinet.com
- Portal for most of the documents, handbooks, guides etc. that are published by Fortinet.
- http://kb.fortinet.com - a searchable database of articles about the configuration and maintenance of Fortinet products.
- https://support.fortinet.com/

DNS Related Information

http://www.dnsstuff.com/tools
http://www.dnstoolbox.com/
http://www.domaintools.com/research/
http://en.wikipedia.org/wiki/List_of_Internet_top-level_domains

IP Address

http://ipchicken.com

Port Scanners

http://www.t1shopper.com/tools/port-scan/

Speed Tests

http://speedof.me/
http://www.speakeasy.net/speedtest/

Email Service

http://mxtoolbox.com/

Regular Expression

http://regexpal.com/

Toolkit Checklist

Print out this checklist to help keep track of what you have and what you need.

Hardware

- ☐ Regular FortiGate Console Cable
- ☐ Proprietary Console Cable(s) for:
- ☐ _____
- ☐ _____
- ☐ USB to Serial Adapter
- ☐ Serial To Ethernet adapter
- ☐ USB Cables:
- ☐ Standard B
- ☐ Mini B
- ☐ Ethernet Cables
- ☐ Ethernet Cable, Crossover
- ☐ RJ45 Coupler

Software

- ☐ Code Editor
- ☐ Terminal Emulator
- ☐ TFTP Server
- ☐ MD5 Checking Tool
- ☐ LDAP Browsing Tool
- ☐ Packet Sniffing Software

Items I thought of myself

(And should email into techdocs@fortinet.com as suggestions)

- ☐ _____
- ☐ _____
- ☐ _____